CLAIMS

What is claimed is

1. A method of securely invoking an access control function, the method comprising the steps of:

receiving a digital signature for the access control function;

generating a mapping of the access control function to the digital signature;

determining that the digital signature is mapped to the access control function based on the mapping when execution of the access control function is requested;

determining whether an executable element matches the access control function based on the digital signature; and

executing the executable element only when the executable element matches the access control function.

2. The method of Claim 1,

wherein a particular class defines an implementation for the access control function;

wherein the step of receiving a digital signature includes the step of receiving a digital signature for the particular class; and

wherein the step of generating a mapping includes generating a mapping between the particular class and the digital signature.

3. The method of Claim 1,

wherein the method further includes the step of detecting that an access control event has occurred; and

wherein the step of retrieving the executable element is performed in response to detecting that the event has occurred.

4. The method of Claim 3,

wherein the method further includes the steps of:

generating a mapping between the access control event and the access control function;

determining that the access control event is mapped to the access control function; and

wherein the step of retrieving the executable element is performed in response to determining that the access control event is mapped to the access control function.

5. The method of Claim 4, further including the step of the executable element returning name-value pairs.

6. The method of Claim 5, wherein the step of the executable element returning name-value pairs includes the executable element returning a hash table that contains the name-value pairs.

7. The method of Claim 1, wherein the method further includes the steps of:

generating a mapping of a plurality of access control functions to digital signatures, wherein the plurality of access control functions include the access control function, wherein one or more classes define an implementation for each of the plurality of access control functions; and

wherein each of the one or more classes belong to a superclass.

8. The method of Claim 7, further including the step of invoking a routine defined by a superclass that collects data to return to a caller of the particular class.

9. The method of Claim 8, wherein the step of executing the executable element includes invoking a routine defined for the superclass.

10. The method of Claim 1, wherein the step of retrieving an executable element includes retrieving byte code.

11. The method of Claim 10, wherein the step of retrieving byte code includes retrieving Java byte code.

12. The method of Claim 1, wherein the step of retrieving an executable element includes a first computer system retrieving byte code transmitted via a local area network from a second computer system.

13. A computer-readable medium carrying one or more sequences of one or more instructions for securely invoking an access control function, the one or more sequences of one or more instructions including instructions which, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving a digital signature for the access control function;

generating a mapping of the access control function to the digital signature;

determining that the digital signature is mapped to the access control function based on the mapping when execution of the access control function is requested;

determining whether an executable element matches the access control function based on the digital signature; and

executing the executable element only when the executable element matches the access control function.

14. The computer-readable medium of Claim 13,

wherein a particular class defines an implementation for the access control function;

wherein the step of receiving a digital signature includes the step of receiving a digital signature for the particular class; and

wherein the step of generating a mapping includes generating a mapping between the particular class and the digital signature.

15. The computer-readable medium of Claim 13,

wherein the computer-readable medium further includes sequences of instructions for performing the step of detecting that an access control event has occurred; and

wherein the step of retrieving the executable element is performed in response to detecting that the event has occurred.

16. The computer-readable medium of Claim 15,

wherein the computer-readable medium further includes sequences of instructions for performing the steps of:

generating a mapping between the access control event and the access control function;

determining that the access control event is mapped to the access control function; and

wherein the step of retrieving the executable element is performed in response to determining that the access control event is mapped to the access control function.

17. The computer-readable medium of Claim 16, further including sequences of instructions for performing the step of the executable element returning name-value pairs.

18. The computer-readable medium of Claim 17, wherein the step of the executable element returning name-value pairs includes the executable element returning a hash table that contains the name-value pairs.

19. The computer-readable medium of Claim 13, wherein the computer-readable medium further includes sequences of instructions for performing the steps of:

generating a mapping of a plurality of access control functions to digital signatures, wherein the plurality of access control functions include the access control function, wherein one or more classes define an implementation for each of the plurality of access control functions; and

wherein each of the one or more classes belong to a superclass.

20. The computer-readable medium of Claim 19, further including sequences of instructions for performing the step of invoking a routine defined by a superclass that collects data to return to a caller of the particular class.

21. The computer-readable medium of Claim 20, wherein the step of executing the executable element includes invoking a routine defined for the superclass.

22. The computer-readable medium of Claim 13, wherein the step of retrieving an executable element includes retrieving byte code.

23. The computer-readable medium of Claim 22, wherein the step of retrieving byte code includes retrieving Java byte code.

24. The computer-readable medium of Claim 13, wherein the step of retrieving an executable element includes a first computer system retrieving byte code transmitted via a local area network from a second computer system.

25. An access control system, comprising:
a processor;
a memory coupled to the processor;
a first mapping that maps each of a set of access control functions to a digital signature of that access control function;
the processor configured to retrieve an executable element in response to a request to execute a first access control function;
the processor configured to determine whether the executable element matches the first access control function based on the digital signature; and
the processor configured to execute the executable element when the executable element matches the first access control function.

26. The access control system of Claim 25,
wherein the set of access control functions are each implemented in a class; and
wherein the first mapping maps a class implementing one of the set of access control functions to a digital signature.

27. The access control system of Claim 25, further comprising:
the processor configured to detect that an access control event has occurred; and
the processor configured to retrieve the executable element in response to detecting that the event has occurred.

28. The access control system of Claim 27, further comprising:
the processor configured to generate a mapping between the access control event and the access control function;
the processor configured to determine that the access control event is mapped to the access control function; and

the processor configured to retrieve the executable element in response to determining that the access control event is mapped to the access control function.

29. The access control system of Claim 28, wherein the executable element returns name-value pairs.

30. The access control system of Claim 29, wherein the executable element returns a hash table that contains the name-value pairs.

31. The access control system of Claim 25,
wherein the processor is configured to generate a mapping of a plurality of access control functions to digital signatures;
wherein the plurality of access control functions include the access control function, wherein one or more classes define an implementation for each of the plurality of access control functions; and
wherein each of the one or more classes belong to a superclass.

32. The access control system of Claim 31, further comprising said processor configured to invoke a routine defined by a superclass that collects data to return to a caller of the particular class.

33. The access control system of Claim 32, wherein said processor is configured to execute the executable element by invoking a routine defined for the superclass.

34. The access control system of Claim 33, wherein said executable element is byte code.

35. The access control system of Claim 34, wherein said byte code includes Java byte code.

36. The access control system of Claim 35, wherein said processor is configure to retrieve an executable element by retrieving byte code transmitted via a local area network.